8)
(AM)

(excerpt translation)

Japanese Pat. Appl. Laid-Open (kokai) No. HEI 06-276221
Laid-Open (kokai) Date: September 30, 1994
Title of the Invention: E-MAIL SYSTEM HAVING A FUNCTION FOR CONFIDENTIAL E-MAIL
Application No.: HEI 05-57124
Application Date: March 17, 1993
Applicant: TOSHIBA CORPORATION
Inventor(s): Miwa YASUTAKA
Int. Cl.^{6} H04L 12/54, 12/58, 9/32

※※※※※※※※※※※※※※※※※※※※※※※※※※※※※

Abstract:
PURPOSE: To provide an e-mail system for safe and certain communication with respect to a confidential mail.

CONFIGURATION: A confidential mail, whose text is enciphered, sent by a confidential mail sending unit 23 in the workstation 2-1 is received by a mail server 1. A confidential mail distributing unit 13 in the mail server 1 deciphers the confidential mail and refers to a registration list 4 so as to discriminate

as to whether the user of the confidential mail destination is registered. If the user is registered, it is discriminated that the user is qualified to receive the confidential mail, and the mail server 1 attaches a registered password of the user to the confidential mail, and sends the confidential mail to the user. The destination workstation 2-n receives the confidential mail. After that, when the user of the workstation wishes to display the received confidential mail, the confidential mail displaying unit 27 deciphers the corresponding confidential mail, and requests the user to input the password. If the input password is identical with that of the confidential e-mail, the text of the confidential mail is displayed.

[0025]

An example of an operation performed in the e-mail system of the present invention will now be described with reference to flow diagrams of FIGS. 4 through 6, and FIG. 7, which is a diagram schematically showing an operation. In particular, in the example, a user (sender) of a workstation 2-1 sends a confidential mail to a user (receiver) of a workstation 2-n.

[0026]

When the user (sender) of the workstation 2-1 intends to send a confidential e-mail to the user

(receiver) of the workstation 2-n, the sender creates a confidential e-mail containing a destination 51 and e-mail text 53, as shown in FIG. 2(a), using a mail creating unit 21 in the workstation 2-1 (step S1 in FIG. 4). At that time, the sender attaches confidential mail identification (ID) data 52 to the created e-mail so as to indicate the created e-mail to be a confidential mail.

[0027]

A confidential mail discriminating unit 22 in the workstation 2-1 discriminates as to whether the e-mail, which is created in the mail creating section 21, is confidential or not based on possession or non-possession of the confidential mail ID data 52 (step S2 in FIG. 4).

[0028]

If it is discriminated that the e-mail is not confidential, a non-illustrated ordinary mail sending unit sends the e-mail as a ordinary mail to a mail server 1 (step S3 in FIG. 4).

[0029]

If it is discriminated that the e-mail is confidential likewise in the illustrated example, a confidential mail sending unit 23 is activated and the e-mail text 53 is enciphered by a enciphering section 231 in the confidential mail sending unit 23 as Operation A in FIG. 7 (step S4 in FIG. 4). The enciphered part of the confidential mail is

highlighted by bias lines in FIG. 7.

[0030]

The confidential mail, which (whose text 53) is enciphered by the enciphering section 231, is sent to the mail server 1 by a sending section 232, as shown in Operation B in FIG. 7 (step S5 in FIG. 4). The e-mail (confidential mail), which is sent by the sending section 232 in the workstation 2-1, is sent to the mail server 1 via a network 3.

[0031]

A receiving unit 11 in the mail server 1 receives the e-mail, which is sent from the workstation 2-1 via the network 3, as shown in Operation C in FIG. 7 (step S11 in FIG. 5). A confidential mail discriminating unit 12 in the mail server 1 discriminates as to whether the e-mail, which is received by the receiving unit 11, is confidential or not based on possession or non-possession of the confidential mail ID data 52 (step S12 in FIG. 5). If it is discriminated that the e-mail is not confidential, the e-mail is sent to the destination by a non-illustrated ordinary mail distributing unit (step S13 in FIG. 5).

[0032]

On the other hand, if it is discriminated that the e-mail is confidential likewise the illustrated example, a confidential mail distributing unit 13 is activated and the text of the e-mail is deciphered

by a deciphering section 131 in the confidential mail distributing unit 13 as shown in Operation D in FIG. 7 (step S14 in FIG. 5).

[0033]

A registration list referring section 132 in the confidential mail distributing unit 13 refers to confidential mail receiving permission registration list 4 based on the destination 51 of the confidential mail, which is deciphered by the deciphering section 131, and notifies a distribution discrimination section 133 of the result of reference (step S15 in FIG. 5). The distribution discrimination section 133 discriminates as to whether a user corresponding to the destination 51 of the confidential mail to be distributed is registered in the confidential mail receiving permission registration list 4 based on the result of reference (step S16 in FIG. 5).

[0034]

The distribution discrimination section 133 discriminates that, if the user corresponding to the destination 51 is not registered, the user is unqualified to received a confidential e-mail and that the e-mail is not sent to the destination 51. In this case, the work station 2-n returns the e-mail and an error message, which notifies that the e-mail is addressed to a wrong destination, to the sender (step S17 in FIG. 5).

[0035]

Conversely, if a user corresponding to the destination 51 of the confidential mail is registered, the distribution discriminating section 133 discriminates that the user is qualified to receive a confidential mail, and activates a password attaching section 134 in the confidential mail distributing unit 13. The password attaching section 134 attaches a password 54 corresponding to the destination 51, which password is registered in the confidential mail receiving permission list 4 and is peculiar to the user, to the confidential mail as shown in Operation D in FIG. 7 (step S18 in FIG. 5).

[0036]

An enciphering section 135 in the confidential mail distributing unit 13 receives the confidential mail, to which the password attaching section 134 has attached the password 54, and enciphers the text 53 and the password 54 in the confidential mail as shown in Operation F in FIG. 7 (step S19 in FIG. 5). A distributing section 136 distributes the enciphered confidential mail to the destination workstation 2-n (step S20 in FIG. 5).

[0037]

A receiving unit 24 in the workstation 2-n receives the confidential mail (e-mail), which has been distributed by the mail server 1, as shown in

Operation H in FIG. 7, and stores the confidential mail in a mailbox peculiar to the destination 51 of the confidential mail (step S21 in FIG. 6).

[0038]

The user of the workstation 2-n logs in using a predetermined log-in name, and thereby a mail display reception section 25 is activated, which displays a received e-mail list on a screen based on the e-mails received and stored in the mailbox peculiar to the user having the log-in name (step S22 in FIG. 6). The received e-mail list includes information about e-mail kind (confidential or ordinary), e-mail sender (sender address), and etc.

[0039]

The user (receiver) of the workstation 2-n selects and assigns an e-mail, of which the receiver wishes to read the text 53, among the received e-mail list on the screen using a mouse. Responsive to the receiver's selection, the mail display reception section 25 receives assignment of the e-mail to be displayed (step S23 in FIG. 6), and activates a confidential mail discriminating unit 26. The confidential mail discrimination unit 26 discriminates as to whether the e-mail to be displayed (assigned to-be-displayed e-mail) is confidential or not based on a possession or non-possession of the confidential mail ID data 52(step S24 in FIG. 6).

[0040]

If the e-mail is not confidential, the text of the e-mail is displayed by a non-illustrated ordinary mail displaying unit as an ordinary e-mail without any dedicated process (step S25 in FIG. 6).

[0041]

On the other hand, if the e-mail is confidential as the illustrated example, a confidential mail displaying unit 27 is activated and a deciphering section 271 in the confidential mail displaying unit 27 deciphers the text 53 and the password 54 of the e-mail as shown in Operation I in FIG. 7 (step S26 in FIG. 6).

[0042]

After the decipherment, a password input requesting section 272 in the confidential mail displaying unit 27 displays a screen to request the logged-in user to input a password (step S27 in FIG. 6).

[0043]

The user inputs the own password in accordance with the password input requesting screen, and whereupon a password collating section 273 in the confidential mail displaying unit 27 collates the user input password with the password 54 previously attached to the assigned to-be-displayed mail (confidential mail), as shown in Operation J in FIG. 7 so as to determine the two passwords are identical

(namely, the user input password is right) (step S28 in FIG. 6).

[0044]

If an unqualified user other than the valid receiver of the confidential e-mail logs in using the log-in name of the valid user and fails to input the right password, the discrimination at step S28 takes "NO" route and it is prohibited to display the confidential e-mail (step S29 in FIG. 6).

[0045]

On the other hand, when the valid receiver of the confidential e-mail inputs the right password, the discrimination at step S28 takes "YES" route and a display section 274 is activated. The display section 274 locks functions of copy and paste, cut and paste, print and etc. At the same time, the display section 27 also locks a function of storing the e-mail in the form of a file (e.g., text file) other than the mail system file (storing operation) (step S30 in FIG. 6). Further, the display section 274 displays the text 53 of the assigned to-be-displayed mail (confidential mail) on the screen as shown in Operation K in FIG. 7 (step S31 in FIG. 6).

[0046]

In the illustrated embodiment, when the mail display reception section 25 in the receiver (destination) workstation 2-n receives a confidential mail as an assigned to-be-displayed

mail, the workstation 2-n deciphers the enciphered text 53 and password 54, requests the receiver to input a password, and then collates the deciphered password 54 with an inputted password. However, the collation manner should by no means limited to that of the example. In alternation, the workstation 2-n requests the receiver to input the password before the deciphering of the text 53 and the password 54, enciphers the receiver input password, and then collates the enciphered password 54 (enciphered in the mail server 1) of the assigned to-be-displayed mail (confidential mail) with the enciphered receiver input password. If the two enciphered password are identical, the enciphered text 53 is deciphered and displayed on the screen. In this case, since the text 53 is not deciphered if the receiver does not input the right password, it is surely possible to prevent a confidential mail from being leaked to a third person or a third party.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-276221
(43)Date of publication of application : 30.09.1994

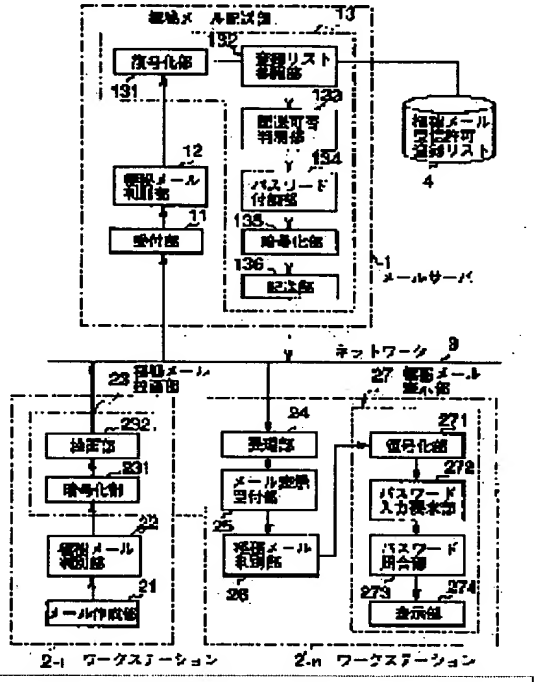
(51)Int.Cl. H04L 12/54
H04L 12/58
H04L 9/32

(21)Application number : 05-057124
(22)Date of filing : 17.03.1993

(71)Applicant : TOSHIBA CORP
(72)Inventor : YASUTAKA MIWA

(54) ELECTRONIC MAIL SYSTEM CONTAINING TOP SECRET MAIL FUNCTION

(57)Abstract:
PURPOSE: To ensure the safe and sure operation of electronic mails of top secret contents.
CONSTITUTION: A top secret mail whose text is ciphered and mailed through a top secret mail mailing part 23 in a work station 2-1 is received by a mail server 1. A top secret mail delivery part 13 of the server 1 decodes the received secret mail and refers to a register list 4 according to the address of the mail. Then the part 13 discriminates the grant of delivery of the mail when the user name of the mail address is registered in the list 4 and adds a password that is registered corresponding to the user name to the mail. These password and the ciphered top secret mail text is delivered to its address. The mail is received at a work station 2-n of the due address. Then, when the user requests the display of the received mail, a top secret mail display part 27 decodes the mail and requests the user to input his password. Then the part 27 displays the mail text when the input password is coincident with the one included in the mail.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平6－276221

(43)公開日　平成6年(1994)9月30日

(51)Int. Cl.[5]	識別記号	庁内整理番号	FI			技術表示箇所
H04L	12/54					
	12/58					
	9/32					
		8732－5K	H04L	11/20	101	B
		8949－5K		9/00		A

審査請求　未請求　請求項の数2　OL　（全10頁）

(21)出願番号　特願平5-57124

(22)出願日　平成5年(1993)3月17日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　安高　みわ
東京都府中市東芝町1番地　株式会社東芝府中工場内

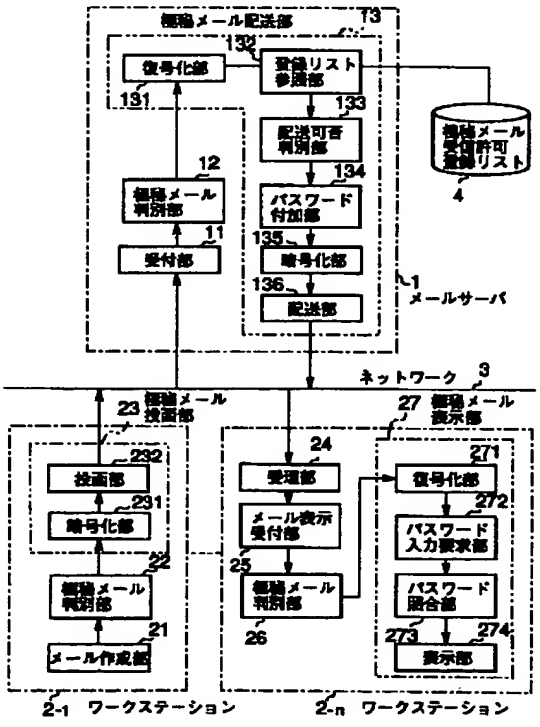
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】極秘メール機能を持つ電子メールシステム

(57)【要約】

【目的】極秘内容のメールに対する安全且つ確実なメール運用を可能とする。

【構成】ワークステーション２-1内の極秘メール投函部２３により投函されたメール本文が暗号化された極秘メールは、メールサーバ１で受付けられる。サーバ１内の極秘メール配送部１３では、同メールを復号化した後、同メールの宛名により登録リスト４を参照し、その宛名のユーザ名が登録されているなら配送可を判別して、そのユーザ名に対応して登録されているパスワードを付加し、このパスワードとメール本文が暗号化された極秘メールを宛先に配送する。この極秘メールは宛先のワークステーション２-nで受理される。その後、受理済みの極秘メールの表示がユーザから要求されると、極秘メール表示部２７では、同メールを復号化した後、ユーザにパスワード入力を要求し、その入力パスワードが同メール中のパスワードに一致しているなら、同メールのメール本文を表示する。



1

【特許請求の範囲】

【請求項１】　電子メールの投函および受理を司る電子メール投函・受理機能を有する複数の第１の処理機器と、前記第１の処理機器から投函された電子メールの受付および配送を司る電子メール受付・配送機能を有する第２の処理機器とを備えた電子メールシステムにおいて、

前記第１の処理機器から極秘メールであることを示す極秘メール識別子が付加された電子メールを投函する際には、同メール中のメール本文を暗号化した後、同メールを極秘メールとして投函する極秘メール投函手段と、

前記極秘メールが受信可能なユーザのユーザ名とそのユーザに固有のパスワードが登録された登録リストと、

前記極秘メール投函手段により投函された前記極秘メールが前記第２の処理機器にて受付けられた際に前記登録リストを参照し、同メールの宛名に一致するユーザ名が登録されている場合だけ、そのユーザ名に固有の前記パスワードを前記登録リストから取り出して同メールに付加し、このパスワードと同メール中の前記メール本文が暗号化された極秘メールを、前記第２の処理機器から宛先の前記第１の処理機器に配送する極秘メール配送手段と、

前記極秘メール配送手段により配送されて前記第１の処理機器で受理された前記極秘メールの画面表示が要求された場合に、外部からのパスワード入力を要求し、この要求に応じて入力されたパスワードが同メール中の前記パスワードに一致した場合だけ、同メール中の前記メール本文の復号化された内容を表示する極秘メール表示手段とを具備することを特徴とする電子メールシステム。

【請求項２】　前記極秘メール表示手段は、表示された前記極秘メールの内容の文字列を対象とする各種操作並びに印刷と、同メールの任意のファイルへの保存とを禁止することを特徴とする請求項１記載の電子メールシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、ワークステーション、パーソナルコンピュータなどの処理機器間で電子メールが授受される電子メールシステムに係り、特に極秘にすべきメール内容の送受信に好適な電子メールシステムに関する。

【０００２】

【従来の技術】一般に電子メールシステムでは、ネットワーク等により結ばれたワークステーション、パーソナルコンピュータなどの処理機器のうちのいずれかに、電子メールの受付および配送を司る電子メール受付・配送機能、即ちメールサーバとしての機能を持たせ、他の処理機器に電子メールの投函および受理を司る電子メール投函・受理機能を持たせることにより実現されている。

【０００３】この種の電子メールシステムでは、電子メール投函・受理機能を持つ処理機器により投函されてメールサーバ（の役割を持つ処理機器）で受付けられた電子メールは、同メールの宛名に従い、その宛先に無条件で配送されるようになっていた。また、この配送された電子メールが、宛先の処理機器で受理された場合、ユーザは特別の入力操作をすることなく、或いは単にログインするだけで、受理された電子メールのメール本文を読む（見る）ことができるようになっていた。したがって、特に極秘にしたいメールでない限りにおいては、ユーザにとって使いやすいものであった。

【０００４】

【発明が解決しようとする課題】しかしながら、上記した従来の電子メールシステムは、極秘の内容のメールに対しては、そのセキュリティは万全ではなかった。即ち、従来の電子メールシステムでは、受理された電子メールの内容は、特別の入力操作をすることなく、或いは単にログインするだけで、誰でも自由に読むことができるため、極秘内容が読まれる虞があった。

【０００５】この発明は上記事情を考慮してなされたものでその目的は、極秘内容のメールに対して安全且つ確実なメール運用が図れる電子メールシステムを提供することにある。

【０００６】

【課題を解決するための手段】この発明は、電子メール投函・受理機能を有する複数の第１の処理機器と、電子メール受付・配送機能を有するメールサーバとしての第２の処理機器とを備えた電子メールシステムにおいて、第１の処理機器から極秘メールであることを示す極秘メール識別子が付加された電子メールを投函する際には、同メール中のメール本文を暗号化した後、同メールを極秘メールとして投函する極秘メール投函手段と、極秘メールが受信可能なユーザのユーザ名とそのユーザに固有のパスワードが登録された登録リストと、上記投函された極秘メールが第２の処理機器にて受付けられた際に上記登録リストを参照し、同メールの宛名に一致するユーザ名が登録されている場合だけ、そのユーザ名に固有のパスワードを登録リストから取り出して同メールに付加し、このパスワードと同メール中のメール本文が暗号化されたメール（極秘メール）を、第２の処理機器（メールサーバ）から宛先の第１の処理機器に配送する極秘メール配送手段と、上記配送された極秘メールが宛先の第１の処理機器で受理された後、その極秘メールの画面表示が要求された場合に、外部からのパスワード入力を要求し、この要求に応じて入力されたパスワードが同メール中のパスワードに一致した場合だけ、同メール中の前記メール本文の復号化された内容を表示する極秘メール表示手段とを備えたことを特徴とするものである。

【０００７】また、この発明は、上記極秘メール表示手段により表示された極秘メールの内容の文字列を対象とする各種操作並びに印刷と、同メールの任意のファイル

への保存とを禁止するようにしたことも特徴とする。

【０００８】

【作用】上記の構成において、極秘内容のメールを送信したい場合、送信者は、メール作成時に、当該メールが極秘メールであることを示す識別子（極秘メール識別子）を付加する。このメール（極秘メール）を第１の処理機器から投函（送信）する際には、極秘メール投函手段により、同メール中のメール本文が暗号化される。この暗号化されたメール本文を持つ極秘メールは、極秘メール投函手段により投函されてメールサーバ（第２の処理機器）に送られ、同メールサーバにより受付けられる。

【０００９】メールサーバでは、受付けた電子メールが極秘メール識別子を持つ場合、即ち極秘メールを受付けた場合、極秘メール配送手段が起動される。すると極秘メール配送手段は、メールサーバにて受付けられた極秘メールのメール本文を一旦復号化した後、登録リストを参照して、同メールの宛名に一致するユーザ名が登録されているか否かをチェックする。

【００１０】もし、登録されていないならば、極秘メール配送手段は、その宛名のユーザへの極秘メールの配送は許可されていないものとして、そのユーザへの配送を行わずに、発信元にエラーメッセージを返す。

【００１１】一方、極秘メールの宛名に一致するユーザ名が登録されているならば、極秘メール配送手段は、そのユーザ名に対応して登録者リストに登録されているパスワードを取り出して極秘メールに付加し、このパスワードと同メール中のメール本文を暗号化した後、メールサーバから宛先の第１の処理機器に配送（送信）する。

【００１２】このようにしてメールサーバ（の極秘メール配送手段）により配送された極秘メールは、宛先の第１の処理機器で受理され、同メールの宛名で示されるユーザに固有のメールボックスに格納される。

【００１３】ここで、受理された極秘メールを表示することがユーザ操作により要求された場合、極秘メール表示手段は、同メール中のパスワードとメール本文を復号化すると共に、表示画面を通してユーザ操作によるパスワード入力を要求する。そして極秘メール表示手段は、この入力要求に従ってユーザ操作により入力されたパスワードと極秘メール中のパスワードとを比較し、両パスワードが一致しているか否か、即ち入力されたパスワードが正しいか否かをチェックする。そして極秘メール表示手段は、正しいパスワードが入力された場合だけ、極秘メールのメール本文を表示する。このとき極秘メール表示手段は、表示された極秘メールの内容の文字列のコピー＆ペースト、カット＆ペースト並びに印刷の機能を抑止する。また極秘メール表示手段は、表示された極秘メールのメールシステム以外のファイル（例えばテキストファイル）への保存の機能も抑止する。

【００１４】以上のようにして、極秘メールは、その宛

先がメールサーバの登録リストに登録された正規のユーザである場合だけ、その宛先に配送されて受理され、しかも受理された極秘メールの内容は、正しいパスワードが入力された場合しか画面表示されず、この表示内容の文字列に対する各種操作、印刷等も禁止されるため、極秘メールの内容を安全に送信することが可能となる。

【００１５】

【実施例】図１はこの発明の一実施例に係る電子メールシステムのブロック構成図である。

【００１６】図１のシステムは、電子メールの受付および配送を司るメールサーバ１と、電子メール投函・受理機能を持つ処理機器、例えばワークステーション（ホスト）２-1，２-2，…２-nと、これらメールサーバ１およびワークステーション２-1～２-nを結ぶネットワーク３とにより構成される。メールサーバ１は、メールサーバ用のメールプログラムを、メールサーバ機能を持たせたい例えばワークステーションにインストールすることにより実現される。同様に、ワークステーション２-1～２-nが有する電子メール投函・受理機能は、対応するメールプログラムを同ステーション２-1～２-nにインストールすることにより実現される。

【００１７】メールサーバ１には、極秘の内容の電子メール（極秘メール）を受信（受理）することが許されているユーザのユーザ名とそのユーザに固有のパスワードが登録された極秘メール受信許可登録リスト４が設けられている。このリスト４は、例えば磁気ディスク装置に格納されており、メールサーバ用のメールプログラムを通してしか参照できないようになっている。図２は、図１のシステムで適用される極秘メールの形式を示す。

【００１８】極秘メールは、ワークステーション２-i（ｉ＝１～ｎ）から送信（投函）される段階では、図２（ａ）に示すように、宛名（宛先アドレス）５１、同メールが極秘メールであることを示す識別子（極秘メール識別子）５２、およびメール本文５３を有する。この極秘メールには、メールサーバ１から送信（配送）される段階では、図２（ｂ）に示すように、パスワード（宛名５１に固有のパスワード）５４が付加される。なお、発信元（のアドレス）等は省略されている。図３は、図１中のメールサーバ１およびワークステーション２-1～２-nの内部の機能構成を示すブロック図である。

【００１９】ワークステーション２-1は、電子メールを作成するためのメール作成部２１、このメール作成部２１で作成された電子メールが極秘メールであるか否かを判別するための極秘メール判別部２２、および極秘メール投函部２３を有する。この極秘メール投函部２３は、極秘メール判別部２２により極秘メールと判別された場合に、そのメール中のメール本文５３（図２参照）を暗号化する暗号化部２３１、および暗号化後の極秘メールを投函する投函部２３２からなる。なお、通常メールの投函部等は省略されている。以上のワークステーション

２-1の構成は、ワークステーション２-nなど他のワークステーションも同様に有しているが、図３では省略されている。

【００２０】メールサーバ１は、ワークステーション２-1～２-nから投函された電子メールの受付を司る受付部１１、この受付部１１にて受付けられた電子メールが極秘メールであるか否かを判別する極秘メール判別部１２、および極秘メール配送部１３を有する。

【００２１】極秘メール配送部１３は、極秘メール判別部１２により極秘メールと判別された場合に、そのメール中のメール本文５３（図２参照）を復号化する復号化部１３１、そのメール中の宛名５１（図２参照）により極秘メール受信許可登録リスト４を参照する登録リスト参照部１３２、および配送可否判別部１３３を有する。配送可否判別部１３３は、登録リスト参照部１３２の参照結果をもとに、極秘メール中の宛名５１で示されるユーザが受信者として許可されているか否か、即ち同メールの配送が可能であるか否かを判別する。

【００２２】極秘メール配送部１３はまた、配送可否判別部１３３により配送可が判別された極秘メールに、登録リスト参照部１３２による参照の結果得られた宛名５１の示すユーザに固有のパスワード５４（図２参照）を付加するパスワード付加部１３４、パスワード５４とメール本文５３を暗号化する暗号化部１３５、および暗号化後の極秘メールを宛名５１の示す宛先に配送する配送部１３６を有する。なお、通常メールの配送部等は省略されている。

【００２３】ワークステーション２-nは、メールサーバ１により配送された電子メールの受理を司る受理部２４、受理された電子メールの表示に対する外部からの要求を受付けるメール表示受付部２５、受付けられた電子メールが極秘メールであるか否かを判別する極秘メール判別部２６、および極秘メール表示部２７を有する。

【００２４】極秘メール表示部２７は、極秘メール判別部２６により極秘メールと判別された場合に、そのメール中のパスワード５４とメール本文５３（図２参照）を復号化する復号化部２７１、およびメール表示要求者に対してパスワードの入力を要求するパスワード入力要求部２７２を有する。極秘メール表示部２７はまた、入力されたパスワードと表示要求された極秘メール中のパスワード５４とを照合するパスワード照合部２７３、および表示部２７４を有する。表示部２７４は、パスワード照合部２７３による照合の結果、正しいパスワードの入力が確認された場合、要求された極秘メールのメール本文５３を表示する。また表示部２７４は、表示された極秘メールのメール本文５３の文字列のコピー&ペースト、カット&ペーストおよび印刷と、メールシステム以外のファイルへの保存を禁止する。以上のワークステーション２-nの構成は、ワークステーション２-1など他のワークステーションも同様に有しているが、図３では省略されている。

【００２５】次に、この発明の一実施例の動作を、ワークステーション２-1のユーザ（送信者）からワークステーション２-nのユーザ（受信者）へ極秘メールを送る場合を例に、図４乃至図６のフローチャートと図７の動作説明図を参照して説明する。

【００２６】ワークステーション２-1のユーザが、ワークステーション２-nのユーザへ、極秘にしたい内容の電子メールを送りたい場合、そのユーザ（送信者）は、ワークステーション２-1内のメール作成部２１を用いて、図２（ａ）に示すような、宛名５１およびメール本文５３を含む電子メール（極秘メール）を作成する（図４ステップＳ１）。この際、送信者は、このメールに、同メールが極秘メールであることを示す極秘メール識別子５２を付加する。

【００２７】ワークステーション２-1内の極秘メール判別部２２は、メール作成部２１により作成された電子メールが極秘メールであるか否かを、極秘メール識別子５２の有無により判別する（図４ステップＳ２）。

【００２８】もし、極秘メールでなければ、その電子メールは通常のメールとして、図示せぬ通常メール投函部によりメールサーバ１に対して投函される（図４ステップＳ３）。

【００２９】一方、この例のように極秘メールであれば、極秘メール投函部２３が起動され、同極秘メール投函部２３内の暗号化部２３１により、このメール中のメール本文５３が図７において符号Ａで示すように暗号化される（図４ステップＳ４）。なお、図７では、メール中の暗号化されている部分に斜線を施してある。

【００３０】そして、暗号化部２３１により（メール本文５３が）暗号化された極秘メールは、投函部２３２により、図７において符号Ｂで示すようにメールサーバ１に対して投函される（図４ステップＳ５）。ワークステーション２-1内の投函部２３２により投函された電子メール（極秘メール）は、ネットワーク３を介してメールサーバ１に送信される。

【００３１】メールサーバ１内の受付部１１は、このネットワーク３を介して送信されたワークステーション２-1からの電子メールを、図７において符号Ｃで示すように受付ける（図５ステップＳ１１）。メールサーバ１内の極秘メール判別部１２は、受付部１１によって受付けられた電子メールが極秘メールであるか否かを、極秘メール識別子５２の有無により判別する（図５ステップＳ１２）。もし、極秘メールでなければ、その電子メールは通常のメールとして、図示せぬ通常メール配送部により宛先に配送される（図５ステップＳ１３）。

【００３２】一方、この例のように極秘メールであれば、極秘メール配送部１３が起動され、同極秘メール配送部１３内の復号化部１３１により、このメール中のメール本文５３が図７において符号Ｄで示すように復号化

される（図５ステップＳ１４）。

【００３３】極秘メール配送部１３内の登録リスト参照部１３２は、復号化部１３１によって復号化された極秘メール中の宛名５１により極秘メール受信許可登録リスト４を参照して、その参照結果を配送可否判別部１３３に通知する（図５ステップＳ１５）。配送可否判別部１３３は、この登録リスト参照部１３２の参照結果により、配送の対象となる極秘メール中の宛名５１に一致するユーザ名が、極秘メール受信許可登録リスト４に登録されているか否かをチェックする（図５ステップＳ１６）。

【００３４】配送可否判別部１３３は、極秘メール中の宛名５１に一致するユーザ名が登録されていないならば、その宛名５１のユーザは極秘メールを受信することが許されていないものとして、そのユーザへの極秘メールの配送不可を判断する。この場合、（誤った宛先への極秘メール送信である旨を示す）エラーメッセージとそのメールとが、ワークステーション２-nから送信者（発信元）に返される（図５ステップＳ１７）。

【００３５】一方、極秘メール中の宛名５１に一致するユーザ名が登録されているならば、配送可否判別部１３３は、そのユーザへの極秘メールの配送可を判断して、極秘メール配送部１３内のパスワード付加部１３４を起動する。これによりパスワード付加部１３４は、登録リスト参照部１３２の参照結果に従い、宛名５１に一致するユーザ名に対応して極秘メール受信許可登録リスト４に登録されている、そのユーザ名に固有のパスワード５４を、図７において符号Ｅで示すように極秘メールに付加する（図５ステップＳ１８）。

【００３６】極秘メール配送部１３内の暗号化部１３５は、パスワード付加部１３４によりパスワード５４が付加された極秘メールを受取り、同メール中のパスワード５４およびメール本文５３を、図７において符号Ｆで示すように暗号化する（図５ステップＳ１９）。この暗号化された極秘メールは、配送部１３６により、図７において符号Ｇで示すように宛先のワークステーション２-nに配送される（図５ステップＳ２０）。

【００３７】ワークステーション２-n内の受理部２４は、メールサーバ１により配送された極秘メール（電子メール）を、図７において符号Ｈで示すように受理し、同メール中の宛名５１に固有のメールボックスに蓄積する（図６ステップＳ２１）。

【００３８】ここで、ワークステーション２-nのユーザが、そのログイン名を用いて所定のログイン操作を行うと、メール表示受付部２５が起動される。メール表示受付部２５は、このログイン名のユーザに固有のメールボックスに蓄積されている受理済み電子メールをもとに、そのメールのリストを画面表示する（図６ステップＳ２２）。このリストには、メールの種別（極秘メールであるか否かなど）と、そのメールの送信者（発信元アドレス）などが含まれている。

【００３９】ワークステーション２-nのユーザ（受信者）は、受理済みメールのリストが表示されると、その内容（メール本文５３）を表示して欲しいメールを、リスト中からマウス等の操作で選択指定する。これにより、メール表示受付部２５は、ユーザからの表示対象メールの指定を受付け（図６ステップＳ２３）、極秘メール判別部２６を起動する。すると極秘メール判別部２６は、メール表示受付部２５にて受付けられた表示対象メール（指定表示対象メール）が極秘メールであるか否かを、極秘メール識別子５２の有無により判別する（図６ステップＳ２４）。

【００４０】もし、極秘メールでなければ、その電子メールは通常のメールであるとして、図示せぬ通常メール表示部により、その本文（メール本文）が無条件で表示される（図６ステップＳ２５）。

【００４１】一方、この例のように極秘メールであれば、極秘メール表示部２７が起動され、同極秘メール表示部２７内の復号化部２７１により、このメール中のパスワード５４およびメール本文５３が図７において符号Ｉで示すように復号化される（図６ステップＳ２６）。

【００４２】極秘メール表示部２７内のパスワード入力要求部２７２は、復号化部２７１による復号化が行われると、上記ログインしたユーザに対してパスワードの入力を要求する画面を表示する（図６ステップＳ２７）。

【００４３】ユーザは、パスワード入力要求画面に従って、自身のパスワードを入力する。すると、極秘メール表示部２７内のパスワード照合部２７３は、入力されたパスワードと指定表示対象メール（極秘メール）中のパスワード５４とを、図７において符号Ｊで示すように照合し、両パスワードが一致しているか否か、即ちユーザが入力したパスワードが正しいか否かをチェックする（図６ステップＳ２８）。

【００４４】もし、指定表示対象メールの正当な受信者でないユーザが、正当な受信者のログイン名を用いてログインしたために、正しいパスワードが入力できなかった場合には、上記ステップＳ２８の判定は「ＮＯ」となり、そのメールのメール本文５３の表示は抑止される（図６ステップＳ２９）。

【００４５】一方、指定表示対象メールの正当な受信者であるユーザが正しいパスワードを入力した場合には、上記ステップＳ２８の判定は「ＹＥＳ」となり、表示部２７４が起動される。すると表示部２７４は、指定表示対象メール（極秘メール）のメール本文５３の表示後の内容の文字列に対する、コピー＆ペースト、カット＆ペーストおよび印刷の機能をロックすると共に、同メールのメールシステム以外のファイル（例えばテキストファイル）への保存（保存操作）の機能をロックする（図６ステップＳ３０）。そして表示部２７４は、指定表示対象メール（極秘メール）のメール本文５３を、図７にお

いて符号Ｋで示すように画面表示する（図６ステップＳ３１）。

【００４６】なお、前記実施例では、受信側（配送先）ワークステーション２-nのメール表示受付部２５で受付けられた表示対象メールが極秘メールである場合に、パスワード５４とメール本文５３を復号化した後、受信者に対してパスワードの入力を要求し、入力パスワードと復号化されたパスワード５４とを照合するものとして説明したが、これに限るものではない。例えば、パスワード５４とメール本文５３を復号化する前にパスワードの入力を要求し、入力パスワードを暗号化して、この暗号化された入力パスワードと、表示対象メール（極秘メール）中の復号化前のパスワード５４（メールサーバ１にて暗号化されたパスワード５４）とを照合し、両パスワードの一致を検出した場合に、メール本文５３を復号化して画面表示するようにしても構わない。この方式では、正しいパスワードが入力されなかった場合には、表示対象メール（極秘メール）中のメール本文５３は復号化されないことから、同メールが第三者へ漏洩されることを一層確実に防止できる。

【００４７】

【発明の効果】以上詳述したようにこの発明によれば、極秘メール識別子が付加された電子メール（極秘メール）のメール本文を暗号化してメールサーバに投函し、この極秘メールを受付けたメールサーバでは、その宛名の示すユーザが、極秘メールの受信者として予め登録リストに登録されている場合に限り、同登録リストに登録されているそのユーザに固有のパスワードを付加して、このパスワードとメール中のメール本文とが暗号化された極秘メールを宛先に配送し、この極秘メールの配送先で同メールが受理された後、同メールの画面表示が要求された際には、外部からのパスワード入力を要求し、入力されたパスワードが同メール中のパスワードに一致した場合だけ、同メール中のメール本文の復号化された内容を表示する構成としたので、極秘内容のメールに対して安全且つ確実なメール運用が図れ、セキュリティ機能が向上する。

【００４８】また、この発明によれば、表示された極秘メールの内容の文字列を対象とする各種操作並びに印刷と、同メールの任意のファイルへの保存とを禁止することにより、第３者への漏洩を一層確実に防止できる。

【図面の簡単な説明】

【図１】この発明の一実施例に係る電子メールシステムのブロック構成図。

【図２】図１のシステムで適用される極秘メールの形式を示す図。

【図３】図１中のメールサーバ１およびワークステーション２-1～２-nの内部の機能構成を示すブロック図。

【図４】ワークステーション２-1による電子メール投函時の処理手順を示すフローチャート。

【図５】メールサーバ１による電子メール受付時の処理手順を示すフローチャート。

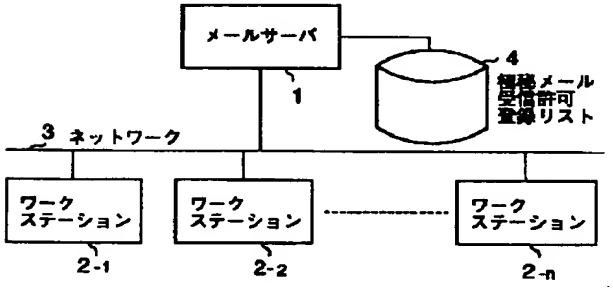
【図６】ワークステーション２-nによる電子メール受理時の処理手順を示すフローチャート。

【図７】ワークステーション２-1からワークステーション２-nへ極秘メールを送る場合の動作を説明するための図。

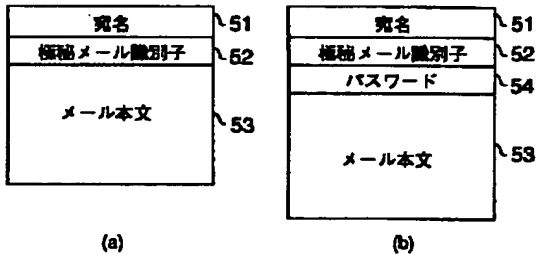
【符号の説明】

１…メールサーバ（第２の処理機器）、２-1～２-n…ワークステーション（第１の処理機器）、３…ネットワーク、４…極秘メール受信許可登録リスト、１１…受付部、１２，２２，２６…極秘メール判別部、１３…極秘メール配送部、２１…メール作成部、２３…極秘メール投函部、２４…受理部、２５…メール表示受付部、２７…極秘メール表示部、１３１，２７１…復号化部、１３２…登録リスト参照部、１３３…配送可否判別部、１３４…パスワード付加部、１３５，２３１…暗号化部、２７２…パスワード入力要求部、２７３…パスワード照合部。

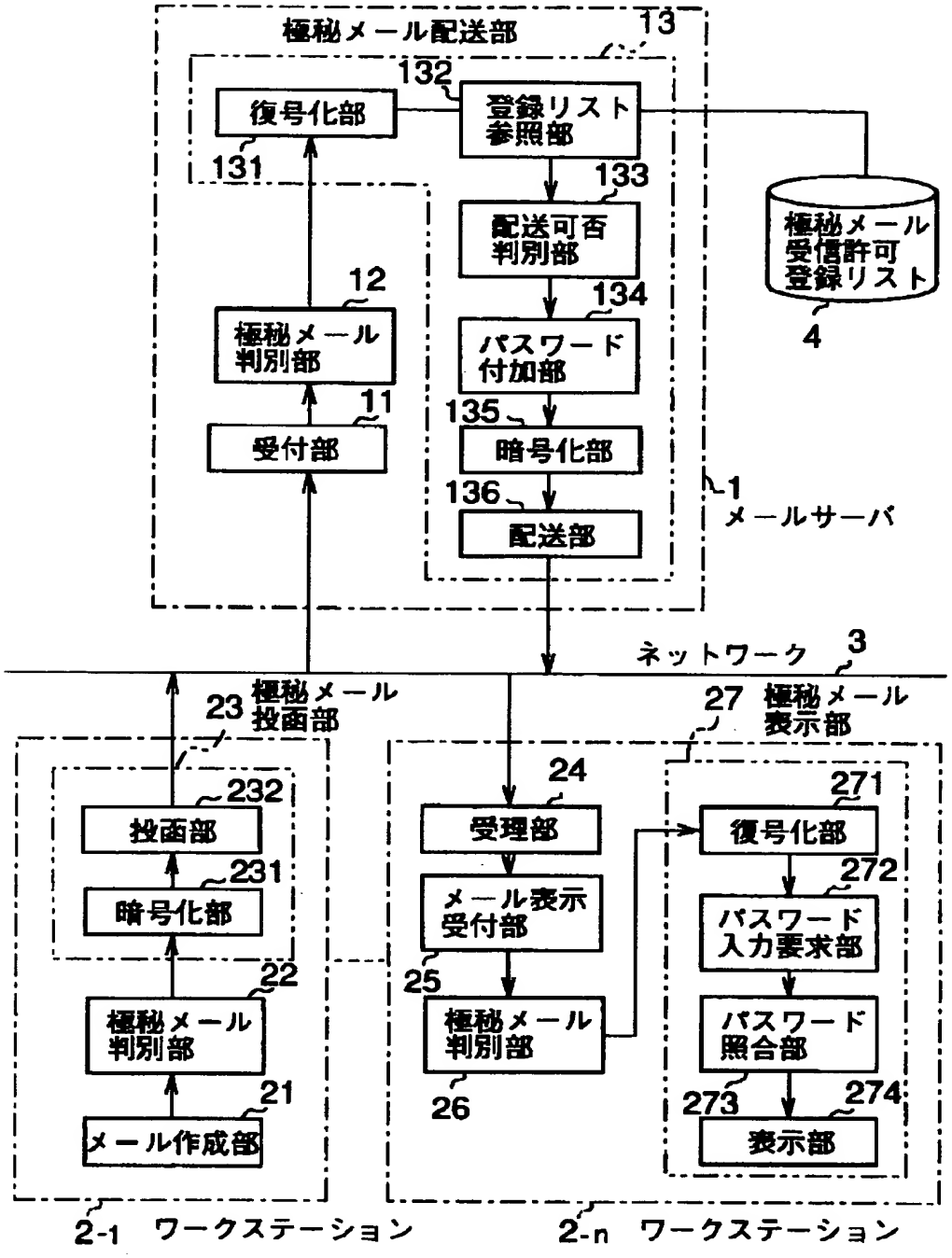
【図１】



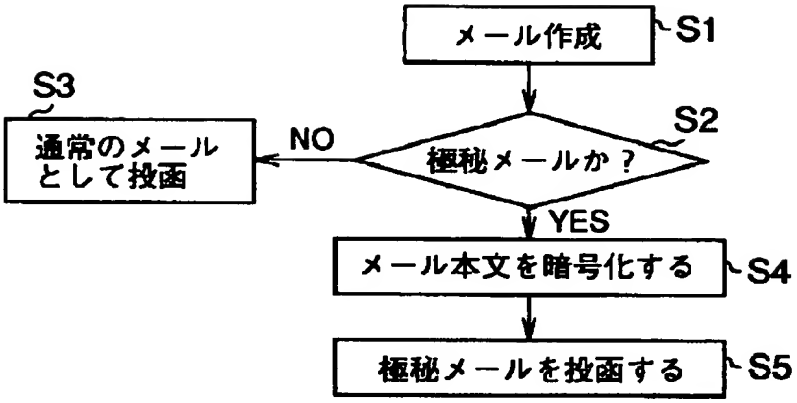
【図２】



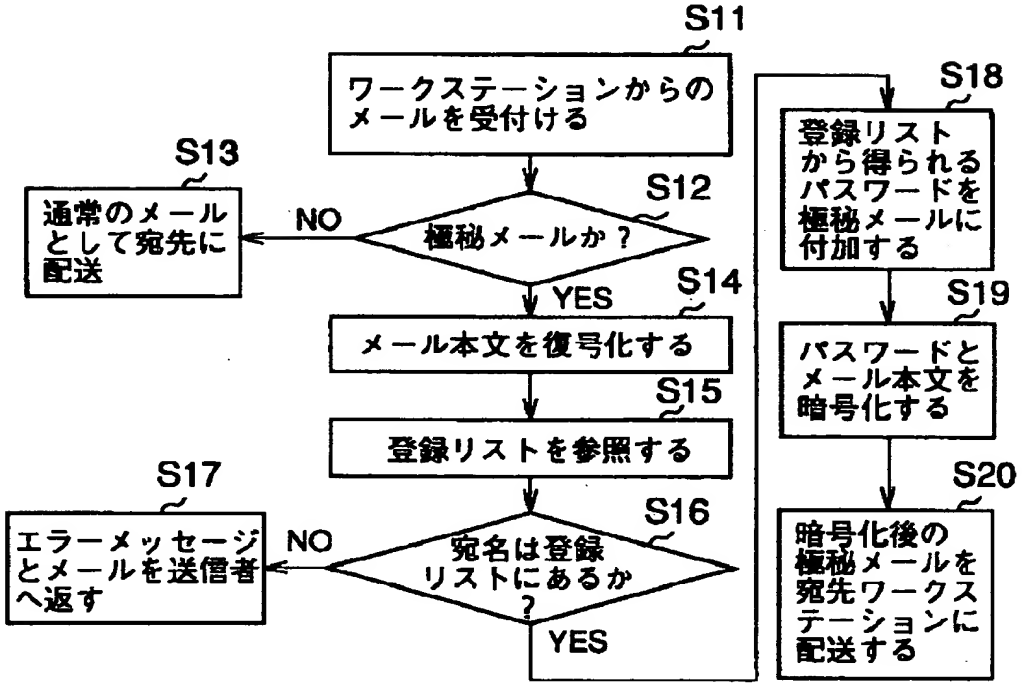
【図３】


極秘メール配送部
13
132
復号化部
登録リスト参照部
131
133
配送可否判別部
極秘メール受信許可登録リスト
4
12
極秘メール判別部
134
パスワード付加部
11
135
受付部
暗号化部
136
配送部
1
メールサーバ
ネットワーク
3
23 極秘メール投函部
27 極秘メール表示部
232
投函部
231
暗号化部
22
極秘メール判別部
21
メール作成部
24
受理部
メール表示受付部
25
極秘メール判別部
26
271
復号化部
272
パスワード入力要求部
パスワード照合部
273
274
表示部
2-1 ワークステーション
2-n ワークステーション

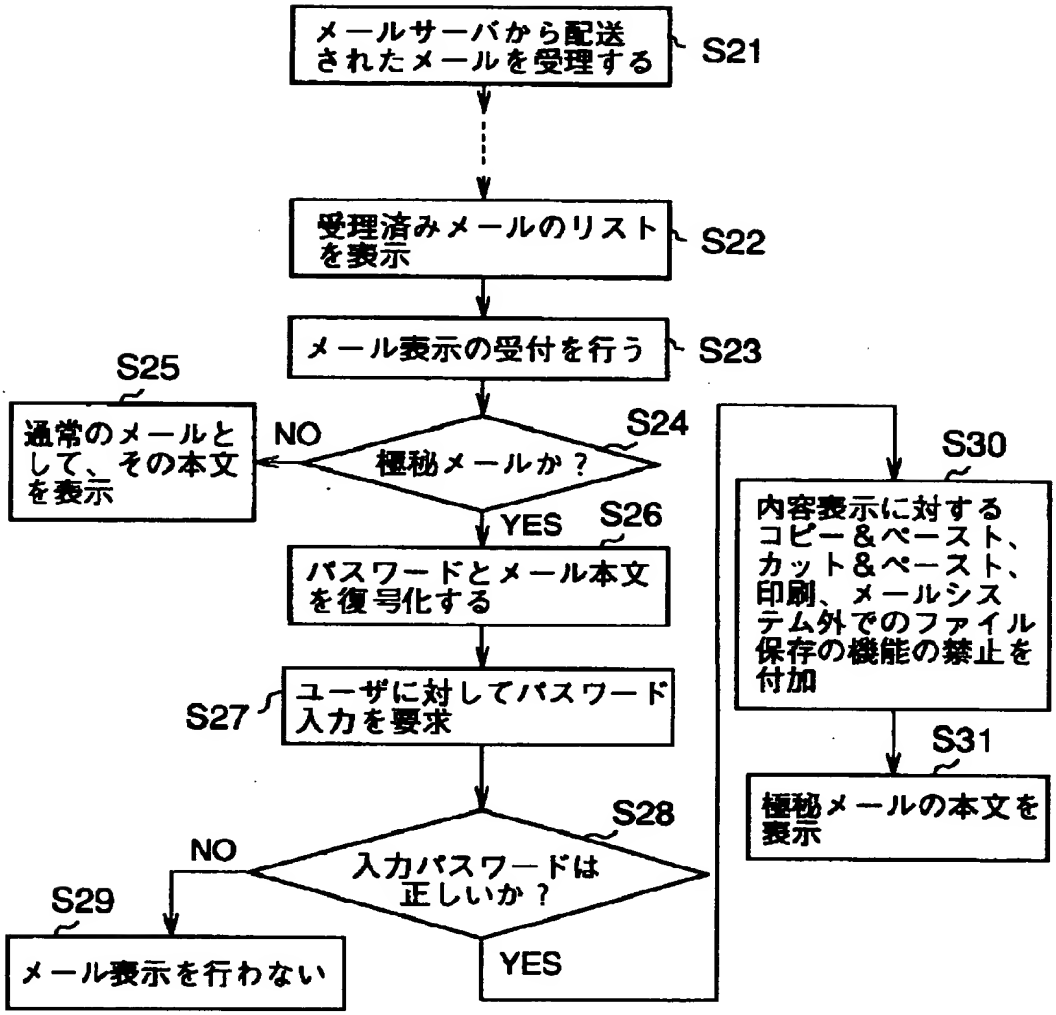
【図４】


メール作成
S1
S3
通常のメール
として投函
NO
極秘メールか？
S2
YES
メール本文を暗号化する
S4
極秘メールを投函する
S5

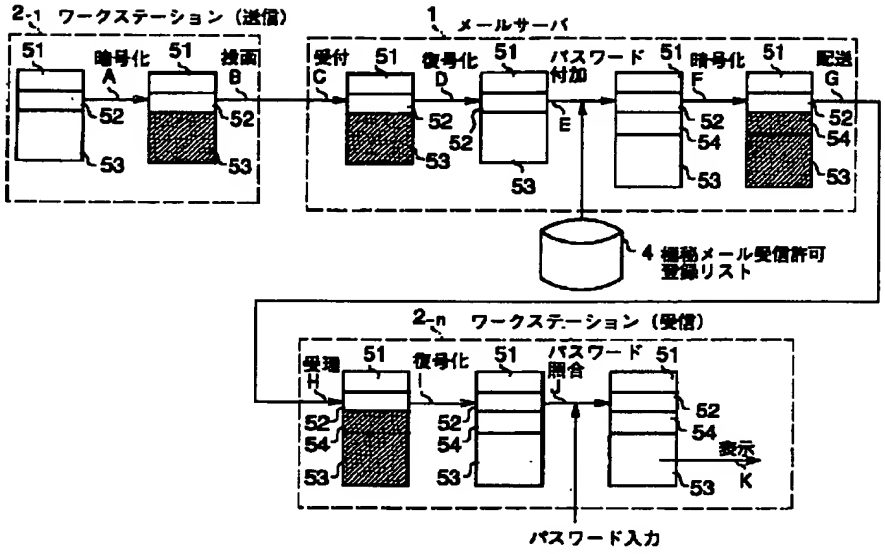
【図５】


S11
ワークステーションからの
メールを受付ける
S13
通常のメール
として宛先に
配送
NO
極秘メールか？
S12
YES
S14
メール本文を復号化する
S15
登録リストを参照する
S17
エラーメッセージ
とメールを送信者
へ返す
NO
宛名は登録
リストにあるか
？
S16
YES
S18
登録リスト
から得られる
パスワードを
極秘メールに
付加する
S19
パスワードと
メール本文を
暗号化する
S20
暗号化後の
極秘メールを
宛先ワークス
テーションに
配送する

【図６】


メールサーバから配送されたメールを受理する
S21
受理済みメールのリストを表示
S22
メール表示の受付を行う
S23
S24
極秘メールか？
NO
S25
通常のメールとして、その本文を表示
YES
S26
パスワードとメール本文を復号化する
S27
ユーザに対してパスワード入力を要求
S28
入力パスワードは正しいか？
NO
S29
メール表示を行わない
YES
S30
内容表示に対するコピー＆ペースト、カット＆ペースト、印刷、メールシステム外でのファイル保存の機能の禁止を付加
S31
極秘メールの本文を表示

【図７】


2-1 ワークステーション（送信）
1 メールサーバ
51
暗号化
A
52
53
検閲
B
受付
C
復号化
D
E
パスワード
付加
F
暗号化
配送
G
54
4 機密メール受信許可
登録リスト
2-n ワークステーション（受信）
受理
H
パスワード
照合
表示
K
パスワード入力